PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2002-208216**
(43)Date of publication of application : **26.07.2002**

(51)Int.Cl. G11B 20/10
G06F 12/14
H04N 5/91

(21)Application number : **2001-004629**
(22)Date of filing : **12.01.2001**

(71)Applicant : **VICTOR CO OF JAPAN LTD**
(72)Inventor : **IBA WATARU**
SUGAWARA TAKAYUKI
UEDA KENJIRO
KUROIWA TOSHIO
HIGURE SEIJI

(54) CONTENTS RECORDING AND REPRODUCING DEVICE

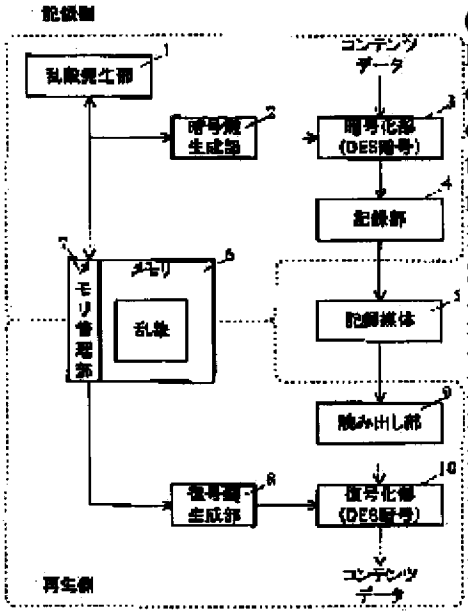

図1.コンテンツ記録再生装置

(57)Abstract:
PROBLEM TO BE SOLVED: To prove a contents recording and reproducing device which can accurately reflect reproduction restrictions in the recording/reproducing of contents with the reproduction restrictions, and can prevent the illegal use of contents.
SOLUTION: Random numbers which are at least part of information constituting the source of a key are generated in a random number generating part 1 at the start-up of a recording operation to a recording medium 5. The random numbers are recorded on a memory 6 through a memory management part 7. The random numbers stored in the memory 6 are erased by powering off processing to the recording and reproducing device or recording operation suspension processing. At the re-power up or a recording operation start-up for a second time, new random numbers are generated in the random number generating part 1, and these random numbers are used as information constituting the source of a new key. An encryption key is generated in an encryption key generating part 2 as information constituting the generated random numbers as the source of the key, and the contents encrypted by using the encryption key are recorded on the recording medium

(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－208216
(P2002－208216A)
(43)公開日　平成14年７月26日(2002.7.26)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ１１Ｂ　20/10		Ｃ１１Ｂ　20/10	Ｈ	５Ｂ０１７
Ｇ０６Ｆ　12/14	３２０	Ｃ０６Ｆ　12/14	３２０Ｂ	５Ｃ０５３
Ｈ０４Ｎ　5/91		Ｈ０４Ｎ　5/91	Ｐ	５Ｄ０４４

審査請求　未請求　請求項の数９　ＯＬ　（全　７　頁）

(21)出願番号　特願2001－4629(P2001－4629)

(22)出願日　平成13年１月12日(2001.1.12)

(71)出願人　000004329
日本ビクター株式会社
神奈川県横浜市神奈川区守屋町３丁目12番地
(72)発明者　猪羽　渉
神奈川県横浜市神奈川区守屋町３丁目12番地　日本ビクター株式会社内
(72)発明者　菅原　隆幸
神奈川県横浜市神奈川区守屋町３丁目12番地　日本ビクター株式会社内
(72)発明者　上田　健二朗
神奈川県横浜市神奈川区守屋町３丁目12番地　日本ビクター株式会社内

最終頁に続く

(54)【発明の名称】　コンテンツ記録再生装置

(57)【要約】
【課題】　再生制限のあるコンテンツに対する記録再生に、その再生制限を正確に反映させることができ、コンテンツの不正利用を防止できるコンテンツ記録再生装置を提供する。
【解決手段】　記録媒体５への記録動作開始時に、乱数発生部１にて、鍵の元になる情報の少なくとも一部となる乱数が発生する。この乱数はメモリ管理部７を介してメモリ６に記録される。本記録再生装置への電源切断処理または記録動作停止処理により、メモリ６内に記憶されていた乱数を消去する。再電源投入時または再度の記録動作開始時には、乱数発生部１にて新たな乱数を発生し、その乱数を新たな鍵の元になる情報とする。暗号鍵生成部２では、発生された乱数を鍵の元になる情報として暗号鍵を生成し、その暗号鍵を用いて暗号化されたコンテンツを記録媒体５に記録する。

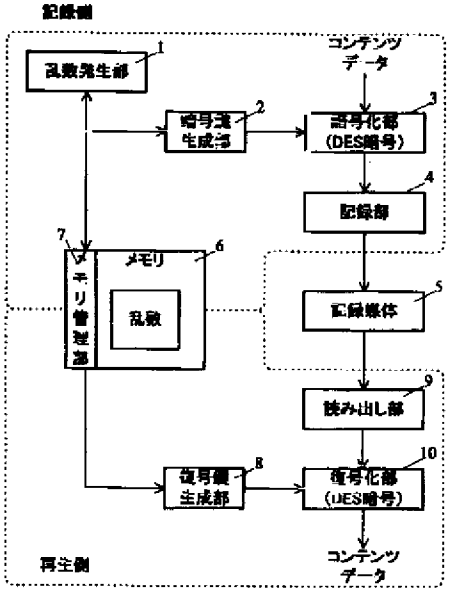

図1.コンテンツ記録再生装置

【特許請求の範囲】
【請求項１】コンテンツを暗号化して記録すると共に、暗号化されたコンテンツを復号化して再生するコンテンツ記録再生装置であって、
乱数を発生する乱数発生手段と、
前記発生された乱数を記憶する乱数記憶手段と、
前記発生された乱数を鍵の元になる情報の少なくとも一部として暗号鍵を生成する暗号鍵生成手段と、
前記生成された暗号鍵を元にコンテンツを暗号化する暗号化手段と、
前記暗号化されたコンテンツを記録媒体に記録する記録手段と、
前記乱数記憶手段から乱数を読み出す乱数読み出し手段と、
前記読み出された乱数を鍵の元になる情報の少なくとも一部として復号鍵を生成する復号鍵情報生成手段と、
前記記録媒体から前記暗号化されたコンテンツを読み出すコンテンツ読み出し手段と、
前記読み出されたコンテンツを、前記生成された復号鍵で復号化する復号化手段と、
本装置に対する特定の処理に連動して、前記乱数記憶手段に記憶された乱数を消去もしくは変更する制御手段と、を備えることを特徴とするコンテンツ記録再生装置。
【請求項２】請求項１記載のコンテンツ記録再生装置において、
前記特定の処理が、本装置に対する電源の投入処理または電源の切断処理であることを特徴とするコンテンツ記録再生装置。
【請求項３】請求項１記載のコンテンツ記録再生装置において、
前記特定の処理が、本装置に対する記録開始処理または記録終了処理であることを特徴とするコンテンツ記録再生装置。
【請求項４】請求項１記載のコンテンツ記録再生装置において、
前記特定の処理が、本装置に対する記録媒体への不正データアクセス処理であることを特徴とするコンテンツ記録再生装置。
【請求項５】コンテンツを暗号化して記録すると共に、暗号化されたコンテンツを復号化して再生するコンテンツ記録再生装置であって、
乱数を発生する乱数発生手段と、
前記発生された乱数を記憶する乱数記憶手段と、
前記発生された乱数を鍵の元になる情報の少なくとも一部として暗号鍵を生成する暗号鍵生成手段と、
前記生成された暗号鍵を元にコンテンツを暗号化する暗号化手段と、
前記暗号化されたコンテンツを記録媒体に記録する記録手段と、
前記コンテンツに対する記録動作が行われた日時に関する記録日時情報を保持する日時情報保持手段と、
前記乱数記憶手段から乱数を読み出す乱数読み出し手段と、
前記読み出された乱数を鍵の元になる情報の少なくとも一部として復号鍵を生成する復号鍵情報生成手段と、
前記記録媒体から前記暗号化されたコンテンツを読み出すコンテンツ読み出し手段と、
前記読み出されたコンテンツを、前記生成された復号鍵で復号化する復号化手段と、
前記日時情報保持手段から前記記録日時情報を読み出し、現在の日時に関する情報である現在日時情報と比較する日時情報読み出し手段と、
前記日時情報読み出し手段での比較結果に応じて、及び本装置に対する特定の処理に連動して、前記乱数記憶手段に記憶された乱数を消去もしくは変更する制御手段と、
を備えることを特徴とするコンテンツ記録再生装置。
【請求項６】請求項５記載のコンテンツ記録再生装置において、
前記特定の処理が、本装置に対する電源の投入処理または電源の切断処理であることを特徴とするコンテンツ記録再生装置。
【請求項７】請求項５記載のコンテンツ記録再生装置において、
前記特定の処理が、本装置に対する記録開始処理または記録終了処理であることを特徴とするコンテンツ記録再生装置。
【請求項８】請求項５記載のコンテンツ記録再生装置において、
前記特定の処理が、本装置に対する記録媒体への不正データアクセス処理であることを特徴とするコンテンツ記録再生装置。
【請求項９】請求項５記載のコンテンツ記録再生装置において、
前記特定の処理が、本装置に対する前記日時情報保持手段の記録日時情報の変更処理または現在日時情報の変更処理であることを特徴とするコンテンツ記録再生装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、コンテンツを暗号化して記録すると共に、暗号化されたコンテンツを復号化して再生するコンテンツ記録再生装置に関する。そして、この発明は特に、再生制限のあるコンテンツに対する記録再生動作に、その再生制限を正確に反映させることのできるコンテンツ記録再生装置を提供することを目的としている。
【０００２】
【従来の技術】著作権を有する映像や音声などのコンテンツにおいて、著作権者の意図により１回だけの視聴を

許可する場合、放送であればコンテンツをCGMS(Copy Generation Management System)を利用しコピー禁止とすることで実現できる。

【０００３】一方、記録媒体に記録したコンテンツにおいて、１回だけの視聴許可を実現するためには、特開2000-149417号公報に開示されているように、コンテンツデータの再生済みの部分に再生済みであることを示す情報を付加するか、または暗号化されたコンテンツであれば、その鍵情報が復号化に使用されたかどうかを示す情報を付加することで実現される。

【０００４】また、再生済みのコンテンツデータの記録領域に関する情報、またはコンテンツデータそのものを消去する方法も開示されている。

【０００５】

【発明が解決しようとする課題】しかし、従来の方法のように、コンテンツデータまたは復号鍵に、それぞれ再生済み、使用済みであることを示す情報を付加するだけでは、実際には、記録媒体上にコンテンツデータは消去されずに残ることになる。仮にコンテンツデータが暗号化されている場合でも、記録媒体上にコンテンツデータと鍵情報とが記録されている限り、それらを取得し不正に利用することは不可能ではない。

【０００６】また、再生済みのコンテンツデータの記録されている領域の情報を消去する、もしくは再生済みのコンテンツデータを消去する場合においても、通常の再生前に、記録媒体を他の機器に接続し他の記録媒体に不正にコピーすることも可能である。例えば、追いかけ再生など、他の記録媒体にはない多くの利点をもつハードディスクを記録媒体とした記録再生装置などでは、ハードディスクを不正に記録再生装置から取り外し、外部のPCに接続すれば、不正にコピーすることも可能である。

【０００７】本発明は、再生制限（例えば、１回視聴可）のあるコンテンツに対する記録再生動作に、その再生制限を正確に反映させることができ、コンテンツの不正利用を防止できるコンテンツ記録再生装置を提供することを目的としている。

【０００８】

【課題を解決するための手段】そこで、上記課題を解決するために本発明は、下記のコンテンツ記録再生装置を提供するものである。

（１）　コンテンツを暗号化して記録すると共に、暗号化されたコンテンツを復号化して再生するコンテンツ記録再生装置であって、乱数を発生する乱数発生手段と、前記発生された乱数を記憶する乱数記憶手段と、前記発生された乱数を鍵の元になる情報の少なくとも一部として暗号鍵を生成する暗号鍵生成手段と、前記生成された暗号鍵を元にコンテンツを暗号化する暗号化手段と、前記暗号化されたコンテンツを記録媒体に記録する記録手段と、前記乱数記憶手段から乱数を読み出す乱数読み出し手段と、前記読み出された乱数を鍵の元になる情報の少なくとも一部として復号鍵を生成する復号鍵情報生成手段と、前記記録媒体から前記暗号化されたコンテンツを読み出すコンテンツ読み出し手段と、前記読み出されたコンテンツを、前記生成された復号鍵で復号化する復号化手段と、本装置に対する特定の処理に連動して、前記乱数記憶手段に記憶された乱数を消去もしくは変更する制御手段と、を備えることを特徴とするコンテンツ記録再生装置。

（２）　上記（１）記載のコンテンツ記録再生装置において、前記特定の処理が、本装置に対する電源の投入処理または電源の切断処理であることを特徴とするコンテンツ記録再生装置。

（３）　上記（１）記載のコンテンツ記録再生装置において、前記特定の処理が、本装置に対する記録開始処理または記録終了処理であることを特徴とするコンテンツ記録再生装置。

（４）　上記（１）記載のコンテンツ記録再生装置において、前記特定の処理が、本装置に対する記録媒体への不正データアクセス処理であることを特徴とするコンテンツ記録再生装置。

（５）　コンテンツを暗号化して記録すると共に、暗号化されたコンテンツを復号化して再生するコンテンツ記録再生装置であって、乱数を発生する乱数発生手段と、前記発生された乱数を記憶する乱数記憶手段と、前記発生された乱数を鍵の元になる情報の少なくとも一部として暗号鍵を生成する暗号鍵生成手段と、前記生成された暗号鍵を元にコンテンツを暗号化する暗号化手段と、前記暗号化されたコンテンツを記録媒体に記録する記録手段と、前記コンテンツに対する記録動作が行われた日時に関する記録日時情報を保持する日時情報保持手段と、前記乱数記憶手段から乱数を読み出す乱数読み出し手段と、前記読み出された乱数を鍵の元になる情報の少なくとも一部として復号鍵を生成する復号鍵情報生成手段と、前記記録媒体から前記暗号化されたコンテンツを読み出すコンテンツ読み出し手段と、前記読み出されたコンテンツを、前記生成された復号鍵で復号化する復号化手段と、前記日時情報保持手段から前記記録日時情報を読み出し、現在の日時に関する情報である現在日時情報と比較する日時情報読み出し手段と、前記日時情報読み出し手段での比較結果に応じて、及び本装置に対する特定の処理に連動して、前記乱数記憶手段に記憶された乱数を消去もしくは変更する制御手段と、を備えることを特徴とするコンテンツ記録再生装置。

（６）　上記（５）記載のコンテンツ記録再生装置において、前記特定の処理が、本装置に対する電源の投入処理または電源の切断処理であることを特徴とするコンテンツ記録再生装置。

（７）　上記（５）記載のコンテンツ記録再生装置において、前記特定の処理が、本装置に対する記録開始処理または記録終了処理であることを特徴とするコンテンツ

記録再生装置。

（８） 上記（５）記載のコンテンツ記録再生装置において、前記特定の処理が、本装置に対する記録媒体への不正データアクセス処理であることを特徴とするコンテンツ記録再生装置。

（９） 上記（５）記載のコンテンツ記録再生装置において、前記特定の処理が、本装置に対する前記日時情報保持手段の記録日時情報の変更処理または現在日時情報の変更処理であることを特徴とするコンテンツ記録再生装置。

【０００９】

【発明の実施の形態】本発明の第１実施例を図１を用いて説明する。この実施例のコンテンツ記録再生装置は、１回視聴可のコンテンツを暗号化して記録し、確実に１回のみ再生可能とするものであり、不正利用に対しては暗号が解けないという強力な方法により視聴制限を保護するものである。

【００１０】このコンテンツ記録再生装置の記録側は、鍵の元になる乱数を生成する乱数発生部１と、その乱数を元に暗号鍵を生成する暗号鍵生成部２と、生成した暗号鍵を元にコンテンツを暗号化する暗号化部３と、暗号化したコンテンツを記録媒体５に記録する記録部４と、鍵の元になる乱数を記憶管理するメモリ６を備えたメモリ管理部７とを有している。

【００１１】再生側は、メモリ６とメモリ管理部７を介してメモリ６から鍵の元になる乱数を読み出し、復号鍵を生成する復号鍵生成部８と、記録媒体５から暗号化されているコンテンツを読み出す読み出し部９と、読み出したコンテンツを前記復号鍵を元に復号化する復号化部１０とを有している。

【００１２】まず、記録動作例を説明する。本記録再生装置の電源が入ったとき、もしくは記録媒体５への記録動作開始時に、乱数発生部１にて、鍵の元になる情報の少なくとも一部となる乱数が発生する。この乱数はメモリ管理部７を介してメモリ６に記録される。本記録再生装置への電源切断処理または記録動作停止処理により、メモリ管理部７はメモリ６内に記憶されていた乱数を消去（または変更）する。再電源投入時または再度の記録動作開始時には、乱数発生部１にて新たな乱数を発生し、その乱数を新たな鍵の元になる情報の少なくとも一部とする。

【００１３】また、記録媒体５上のデータに不正なアクセス処理が行われた場合にも、メモリ管理部７ではメモリ６内に記憶されていた乱数を消去（または変更）し、再度乱数発生部１にて、新たな乱数を発生させる。

【００１４】暗号鍵生成部２では、乱数発生部１で発生された乱数を鍵の元になる情報の少なくとも一部として暗号鍵を生成する。一般的に暗号鍵の生成では、ハッシュ関数を利用し、大きな情報量（ビットサイズ）のデータから、必要な情報量（ビットサイズ）を得る。

【００１５】暗号鍵生成部２にて生成した暗号鍵を用いて暗号化部３にてコンテンツの暗号化を行う。暗号化方法には様々な方法が知られているが、通常映像及び音声など転送速度を重視する場合は共通鍵暗号方式を利用することが多い。暗号化部３では共通鍵暗号方式のDES暗号を利用してコンテンツデータを暗号化するとすれば、64ビット（うち8ビットはパリティビット）の鍵が必要になる。暗号化部３で暗号化されたコンテンツは記録部４にて変調され、記録媒体５に記録される。記録媒体５は、光ディスク、磁気テープ、ハードディスク、固体メモリなどディジタル情報を記録可能な記録媒体であればよい。

【００１６】次に、再生動作例を説明する。再生時には記録媒体５より、暗号化されているコンテンツを読み出し部９にて読み出す。読み出し部９には、記録媒体が光ディスクであれば光ピックアップ、磁気テープであれば磁気ヘッドなど、使用する記録媒体に応じた読み出し手段を用いる。

【００１７】復号鍵生成部８では、メモリ６を管理するメモリ管理部７を介し、メモリ内に記録されている乱数を読み出し、この乱数を鍵の元になる情報の少なくとも一部として復号鍵を生成する。このとき暗号化及び復号化に共通鍵暗号方式が使用されていれば、復号鍵生成部８での処理は暗号鍵生成部２と等しくなる。復号化部１０では生成した復号鍵を元にコンテンツデータを復号化する。

【００１８】このように、本コンテンツ記録再生装置によって記録媒体にコンテンツを記録すれば、コンテンツデータ自身を消去または変更することなく、容易に１回視聴可のコンテンツとして設定することが可能となる。また、鍵の元になる情報の少なくとも一部である乱数は、本コンテンツ記録再生装置に対して不正な動作を行えば消去または変更されてしまうため、ハードディスク記録再生装置等で、記録後、視聴前に記録再生装置から他のPC等を用いてコピーをしようとしても、鍵が消去または変更されてしまうため暗号を解読することができない。

【００１９】従って、本コンテンツ記録再生装置は、再生制限（例えば、１回視聴可）のあるコンテンツに対する記録再生動作に、その再生制限を正確に反映させることができ、コンテンツの不正利用を防止できる。

【００２０】次に、本発明の第２実施例を図２を用いて説明する。コンテンツ記録再生装置の記録側は、鍵の元になる乱数を生成する乱数発生部１と、その乱数を元に暗号鍵を生成する暗号鍵生成部２と、生成した暗号鍵を元にコンテンツを暗号化する暗号化部３と、暗号化したコンテンツを記録媒体５に記録する記録部４と、鍵の元になる乱数を記憶管理するメモリ６を備えたメモリ管理部７とを有している。さらに、記録側は、時計により年、月、日、時、分、秒の日時情報が取得可能であり、

前記コンテンツに対する記録動作が行われた日時に関する記録日時情報を保持する日時情報管理部１１を有している。この日時情報管理部１１は、前記記録日時情報を読み出し、現在の日時に関する情報である現在日時情報と比較する機能を備えている。

【００２１】再生側は、メモリ６とメモリ管理部７を介してメモリ６から鍵の元になる乱数を読み出し、復号鍵を生成する復号鍵生成部８と、記録媒体５から暗号化されているコンテンツを読み出す読み出し部９と、読み出したコンテンツを前記復号鍵を元に復号化する復号化部１０とを有している。

【００２２】まず、記録動作例を説明する。本記録再生装置の電源が入ったとき、もしくは記録媒体５への記録動作開始時に、乱数発生部１にて、鍵の元になる情報の少なくとも一部となる乱数が発生する。この乱数はメモリ管理部７を介してメモリ６に記録される。本記録再生装置への電源切断処理または記録動作停止処理により、メモリ管理部７はメモリ６内に記憶されていた乱数を消去（または変更）する。再電源投入時または再度の記録動作開始時には、乱数発生部１にて新たな乱数を発生し、その乱数を新たな鍵の元になる情報の少なくとも一部とする。

【００２３】また、記録媒体５上のデータに不正なアクセス処理が行われた場合にも、メモリ管理部７ではメモリ６内に記憶されていた乱数を消去（または変更）し、再度乱数発生部１にて、新たな乱数を発生させる。

【００２４】さらに、日時情報管理部１１で管理する日時情報によってメモリ管理部７を介して、メモリ６内の乱数を消去（または変更）することができる。日時情報管理部１１は、保持している記録日時情報を読み出し、その記録日時情報を現在日時情報と比較し、既にメモリ６内に記録された乱数が特定の時間が経過したと判断した場合には、メモリ管理部７を介して、その乱数を消去（または変更）する。

【００２５】また、外部から不正に日時情報管理部１１内の時計の日時設定を変更した場合にも、既にメモリ６内に記録された乱数を消去（または変更）することができる。変更する場合は、再度、乱数発生部１にて新たな乱数が発生する。

【００２６】暗号鍵生成部２にて生成した暗号鍵を用いて暗号化部３にてコンテンツの暗号化を行う。暗号化方法には様々な方法が知られているが、通常映像及び音声など転送速度を重視する場合は共通鍵暗号方式を利用することが多い。暗号化部３では共通鍵暗号方式のDES暗号を利用してコンテンツデータを暗号化するとすれば、64ビット（うち8ビットはパリティビット）の鍵が必要になる。暗号化部３で暗号化されたコンテンツは記録部４にて変調され、記録媒体５に記録される。記録媒体５は、光ディスク、磁気テープ、ハードディスク、固体メモリなどディジタル情報を記録可能な記録媒体であればよい。

【００２７】復号鍵生成部８では、メモリ６を管理するメモリ管理部７を介し、メモリ内に記録されている乱数を読み出し、この乱数を鍵の元になる情報の少なくとも一部として復号鍵を生成する。このとき暗号化及び復号化に共通鍵暗号方式が使用されていれば、復号鍵生成部８での処理は暗号鍵生成部２と等しくなる。復号化部１０では生成した復号鍵を元にコンテンツデータを復号化する。

【００２８】このように、本コンテンツ記録再生装置によって記録媒体にコンテンツを記録すれば、コンテンツデータ自身を消去または変更することなく、容易に１回視聴可のコンテンツとして設定することが可能となる。また、鍵の元になる情報の少なくとも一部である乱数は、本コンテンツ記録再生装置に対して不正な動作を行えば消去または変更されてしまうため、ハードディスク記録再生装置等で、記録後、視聴前に記録再生装置から他のPC等を用いてコピーをしようとしても、鍵が消去または変更されてしまうため暗号を解読することができない。

【００２９】従って、本コンテンツ記録再生装置は、再生制限（例えば、１回視聴可）のあるコンテンツに対する記録再生動作に、その再生制限を正確に反映させることができ、コンテンツの不正利用を防止できる。

【００３０】さらに、本コンテンツ記録装置では、日時情報を元に鍵の元になる情報の乱数を消去または変更することで、１回視聴可のコンテンツだけでなく、ある特定時間内のみ再生可能とするコンテンツに対しても、著作権者の意図を反映した形で記録・再生することができる。また、そのとき不正に日時情報が変更された場合においても、メモリ内の乱数を消去または変更することで、コンテンツを不正利用から保護することができる。

【００３１】なお、上記第１、第２実施例において、ユーザーから特別な理由によってコンテンツデータを再生不可能な状態にしたい要求があった場合に、ボタンやリモコン、ネットワークによる通信手段などのユーザーインターフェースによって、メモリ６内に記憶された乱数を積極的に消去もしくは変更しても良い。また、課金に関する情報を元に、メモリ６内に記憶された乱数を消去もしくは変更しても良い。さらには、再生回数に応じて、メモリ内に記憶された乱数を消去もしくは変更しても良い。

【００３２】

【発明の効果】以上の通り、本発明のコンテンツ記録再生装置は、下記の効果を有する。

（イ）本コンテンツ記録再生装置によって記録媒体にコンテンツを記録すれば、コンテンツデータ自身を消去または変更することなく、容易に再生制限（例えば１回視聴可）付きのコンテンツとして設定することが可能となる。また、鍵の元になる情報の少なくとも一部である乱

数は、本コンテンツ記録再生装置に対して特定の動作を行えば消去または変更されてしまうため、例えば、ハードディスク記録再生装置等で、記録後、視聴前に記録再生装置から他のPC等を用いてコピーをしようとしても、鍵が消去または変更されてしまうため暗号を解読することができない。

【００３３】従って、本コンテンツ記録再生装置は、再生制限（例えば、１回視聴可）のあるコンテンツに対する記録再生動作に、その再生制限を正確に反映させることができ、コンテンツの不正利用を防止できる。

（ロ）本コンテンツ記録装置において、日時情報を元に鍵の元になる情報の乱数を消去または変更するようにすれば、１回視聴可のコンテンツだけでなく、ある特定時間内のみ再生可能とするコンテンツに対しても、著作権者の意図を反映した形で記録・再生することができる。また、そのとき不正に日時情報が変更された場合においても、鍵の元になる情報の乱数を消去または変更することで、コンテンツを不正利用から保護することができる。

【図面の簡単な説明】

【図１】第１実施例を示すブロック図である。

【図２】第２実施例を示すブロック図である。

【符号の説明】

１　乱数発生部
２　暗号鍵生成部
３　暗号化部
４　記録部
５　記録媒体
６　メモリ
７　メモリ管理部
８　復号鍵生成部
９　読み出し部
１０　復号化部
１１　日時情報管理部

【図１】

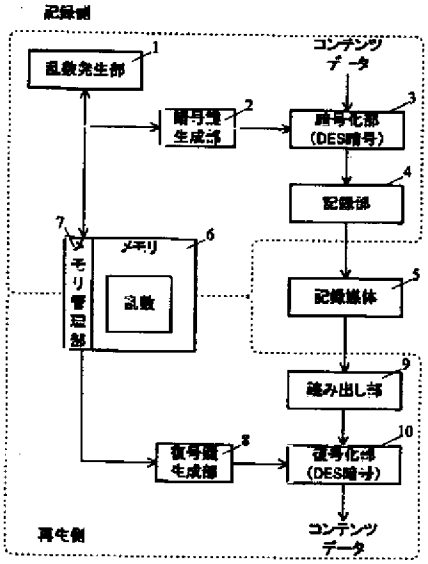

図1.コンテンツ記録再生装置

【図２】

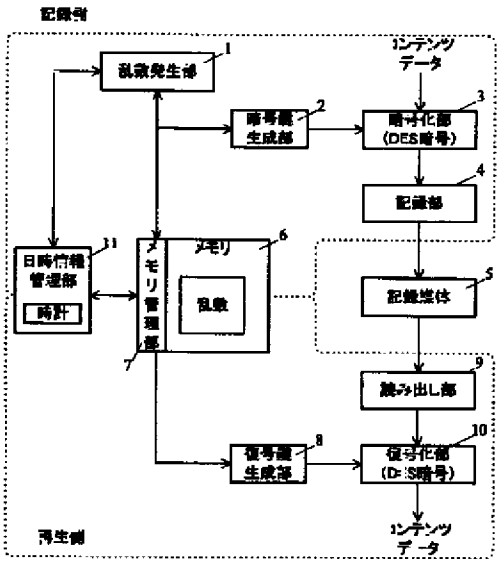

図2.コンテンツ記録再生装置

フロントページの続き

(72)発明者　黒岩　俊夫
神奈川県横浜市神奈川区守屋町３丁目12番地　日本ビクター株式会社内

(72)発明者　日暮　誠司
神奈川県横浜市神奈川区守屋町３丁目12番地　日本ビクター株式会社内

Fターム(参考) 5B017 AA07 BA07 BB10 CA15
5C053 FA13 FA23 JA21 KA01 KA24
5D044 AB05 AB07 BC01 BC04 CC04
DE17 DE50 GK12 GK17